REMARKS

By this Amendment, claims 79, 110, 111, 115 and 117 have been amended. Claims 1, 18-21, 72-84 and 109-131 are pending in this patent application. Reconsideration of the rejections in view of the remarks below is requested.

The Office Action rejected claims 79, 82-84 and 112-114 under 35 U.S.C. §102(b) as being anticipated by U.S. Patent No. 5,214,702 to Fischer ("Fischer"). Applicant respectfully traverses the rejection, without prejudice.

Applicant submits that the cited portions of Fischer fail to at least disclose a method of enforcing a security policy in a cryptographic system, said policy including controlling use of a public key, said method comprising providing a recipient with a message containing rules of said system and with a secure hardware device containing an inactive form of said public key, wherein said public key cannot be obtained from said secure hardware device, and, in response to said recipient digitally signing said message, activating said public key in said secure hardware device, as recited in claim 79.

The cited portions of Fischer appear to describe a party B creating a certificate for a party A. The certificate is an electronic message which is signed by a party (e.g., party B) and which contains, either explicitly or implicitly, a reference to the public-key which is being certified (e.g., party A's public key) and the identity of the public key's owner. See, e.g., Fischer, col. 4, lines 3-8. To form the certificate, party B takes party A's public key, creates a certificate and then digitally signs it using party B's private key. A recipient of the certificate formed by party B can use party B's public key to verify party B's signature.

Applicant respectfully submits that the Office Action has failed to establish that these cited portions of Fischer disclose a secure hardware device containing an inactive form of said public key, wherein said public key cannot be obtained from said secure hardware device. For example, there appears to be no reference to a secure hardware device in the cited portions of Fischer. Even if there were such a disclosure (which Applicant does not concede), there is no reference to an inactive form of a public key or that the public key cannot be obtained from the secure hardware device. At most there is merely a reference to a normally operable and available public key. There is no indication that party A's public key or party B's public key is inactive or unobtainable, whether the public key is in party B's certificate or not.

Further, there appears to be no reference in the cited portions of Fischer to a message containing rules of a system. There is not even a reference to rules, let alone rules of a system in those cited portions. If the certificate formed by party B is alleged to be the message containing rules, then there is no indication of a recipient of that certificate digitally signing that certificate upon which the public key in the secure hardware device is activated. The recipient of the certificate formed by party B, if desired, merely decrypts the signature to that certificate to verify that party B signed the certificate.

Even if the cited portions of Fischer disclosed something occurring in response to a recipient digitally signing the message as claimed (which Applicant does not concede), Applicant respectfully submits that the Office Action has failed to establish that these cited portions of Fischer disclose activating said public key in said secure hardware device. There is not even a reference to activating a public key in these cited portions, let alone activating a public key in a secure hardware device.

The Office Action refers to col. 12, lines 53-60 and col. 14, lines 26-39 of Fischer as disclosing the providing aspect of claim 79. Col. 12, lines 53-60 of Fischer provides:

> When a party B in a ladder of certifications creates an authorizing certificate for party A, the certificate includes a specification of A's identity together with A's public encryption signature/key. Additionally, the certificate indicates the authority, capabilities and limitations which B wishes to grant A. By granting this certificate B explicitly assumes responsibility for both A's identity and authority.

Further, col. 14, lines 26-39 of Fischer provides:

> Additionally, if utilized in an organization, dealing with extremely sensitive business or military information, clearance levels may also be defined in the certificate. In this fashion, a certificate may specify the exact security level of the person who authorized a signed message.
>
> Additionally, each certification may specify the monetary limit, i.e., the maximum amount of money value which the certifiee is authorized to deal with. The monetary limit must not of course exceed the limit in the certifier's own certificate to insure that the certifier does not delegate more than he is allowed to handle. Such a limitation is easily enforced when a recipient receives the set of certificates.

However, there is no reference in those cited portions to a secure hardware device containing an inactive form of a public key, wherein the public key cannot be obtained from said secure hardware device, as recited in claim 79. Further, there appears to be no reference in those cited portions to providing a recipient with a message containing rules of said system which the recipient digitally signs. Those cited portions appear merely to specify certain characteristics of party A.

The Office Action then refers to col. 18, lines 46-64 and col. 19, line 67 to col. 20, line 67 of Fischer as disclosing the activating aspect of claim 79. Col. 18, lines 46-64 provide that:

> Having selected his own certificate with which to sign A's certificate, B at 106 utilizes the certificate 108 with the associated public key 110 to create a signature of a new certificate 112. As in FIG. 2, the signature is created using an object (A's certificate 116) and a certificate (B's certificate 108). B's secret private key is utilized in the decrypt operation to create the signature 112 of the new certificate 116 and the signature packet 114 of B's signature becomes part of A's new certificate packet.
>
> Focusing on the certificate for A which is constructed using information about A specified by B, B builds the certificate by utilizing the public aspect of A's public key as provided by A via line 103. B also sets forth A's full name, A's title and other important statistics such as his address, and telephone number. B may also include a comment to go with the certification which will be available to any person in the future who needs to examine A's certificate.

Further, col. 19, line 67 to col. 20, line 67 provide that:

> B additionally incorporates his own public key has into the certificate which identifies B as the primary sponsor of A's certificate. As the creator of A's certificate, it is contemplated that B will have the authority to cancel A's certificate. B may also designate other parties who may sign A's certificate to grant various types of authority to A.
>
> Other fields may be included in the certificate. For example, the current date and time which reflects the moment of the initial creation of the certificate. As indicated in FIG. 5, the complete certificate consists of a certificate packet with includes the certificate 116 for A and the signature packet 114 of B's signature to A's certificate.
>
> B's signature and the hierarchy of all certificates and signatures which validate it are kept by A and sent along whenever A uses his certificate. It is contemplated that B or other parties may create several certificates for A. For example, one certificate might allow A to reliably identify himself with no further designated authority. Another certificate might allow authorization to A of certain limited money amounts without requiring any cosignatures. A third might allow authorization for larger amounts but require one or more cosignatures. Still another might allow A to subcertify other persons according to still different money and/or authority limitations and/ or co-signature specifications.
>
> Assuming that B has created a certificate for A as shown in FIG. 5, if B requires no cosigners then the certificate is complete. However, the certificate which empowered B to create A's certificate may have required that B have cosigners. There may be one or more joint signature and/or counter signature requirements.
>
> FIG. 6 exemplifies the steps taken by party C to jointly certify the certificate of A. The requirement to have a joint signer would be specified in B's own certificate. In this case, a transmitted object (in this case A's

> new certificate) signed with B's certificate would be rejected by a recipient if C's joint signature is not also present on the object.
>
> As shown in FIG. 6, if such a joint signature is required, a copy of B's certificate for A is sent (120) to C who must jointly sign the certificate (132). C then (122) examines A's certificate and verifies that the public key of the certificate actually belongs to A in accordance with process outlined in conjunction with FIG. 3.
>
> C then examines the signed attributes and authorizations set forth in the certificate including the assigned monetary level, trust level, etc. C then, upon concluding that all the fields in B's certificate for A are appropriate, selects his own certificate with which to perform the signature 126. With his own certificate 128, C signs B's certificate of A 132 (130). Once C signs his certificate his signature appears essentially parallel with B's signature and any other cosigners as shown at 134 and 136 of FIG. 6. Thus, it is important that C exercise as much caution as B when approving A's certificate. Once A's certificate is created no cosigner may change the certificate for to do so would create essentially a different object to which none of the previous signatures would apply. If C does not approve the certificate he must avoid signing it, and should have a different certificate constructed and re-signed by all necessary parties. After C adds his joint certificate to B's certificate of A, A's certificate packet consists of the certificate for A 132, B's signature packet for A's certificate 134 and finally C's signature packet for A's certificate 136.

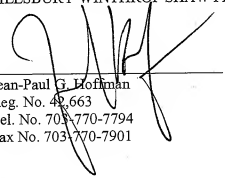
However, there is no reference in those cited portions to, in response to said recipient digitally signing said message, activating said public key in said secure hardware device, as recited in claim 79. The cited portions above refer to party B signing a certificate certifying party A. There is no disclosure of party B signing a message containing rules of a system. Moreover, there is no disclosure that such signing by party B activates a public key in a secure hardware device. Rather, party B has access to an active and available public key, whether party B's or party A's, all along. If party B didn't, party B surely couldn't certify party A's public key or sign the certificate using party B's private key.

Therefore, for at least the above reasons, the cited portions of Fischer fail to disclose all the features recited by claim 79. Claims 82-84 and 112-114 depend from claim 79 and are thus patentable at least for the same reasons as claim 79, as well as for the additional features recited therein. As a result, Applicant respectfully submits that the rejection under 35 U.S.C. §102(b) of claims 79, 82-84 and 112-114 based on Fischer should be withdrawn and the claims be allowed.

All rejections having been addressed, it is respectfully submitted that the present application is in condition for allowance. If questions relating to patentability remain, the Examiner is invited to contact the undersigned to discuss them.

Should any fees be due, please charge them to our deposit account no. 03-3975, under our order no. 061047/0264493. The Commissioner for Patents is also authorized to credit any over payments to the above-referenced deposit account.

Respectfully submitted,
PILLSBURY WINTHROP SHAW PITTMAN LLP



Jean-Paul G. Hoffman
Reg. No. 42,663
Tel. No. 703-770-7794
Fax No. 703-770-7901

P. O. Box 10500
McLean, VA 22102
(703) 770-7900